Listing of Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Previously Presented) A method of verifying an age of a bearer of a document, said method comprising:

receiving, at a processor, first digital data corresponding to an age indicator, the first digital data being obtained from auxiliary data steganographically embedded in the document;

receiving second digital data corresponding to a biometric indictor, the second digital data being obtained from auxiliary data steganographically embedded in the document;

receiving third digital data corresponding to a biometric sample, wherein the biometric sample corresponds to the bearer; and

verifying the bearer's age when: i) the first digital data indicates that the bearer is at least as old as a predetermined age, and ii) the second digital data and the third digital data correspond.

2. (Original) The method of claim 1, further comprising interrogating a data repository with the biometric indictor to obtain the second digital data.

3. (Original) The method of claim 2, further comprising interrogating the data repository with the age indictor to obtain the first digital information.

4. (Original) The method of claim 2, wherein the second digital data comprises a biometric template associated with the bearer.

5. (Previously Presented) The method of claim 4, wherein the biometric template includes information associated with at least one of the bearer's fingerprint, face map, hand geometry, iris, retina, DNA, voiceprint or vein pattern.

6. (Original) The method of claim 1, wherein the third digital data is received through a network.

7. (Original) The method of claim 6, wherein the network comprises the internet.

8. (Original) The method of claim 1, wherein the biometric indicator comprises a biometric template.

9. (Previously Presented) The method of claim 8, wherein the biometric template includes information associated with at least one of the bearer's fingerprint, face map, hand geometry, iris, retina, DNA, voiceprint or vein pattern.

10. (Original) The method of claim 1, wherein the third digital data further comprises a timestamp.

11. (Original) The method of claim 4, wherein the auxiliary data comprises plural bits of data and wherein the biometric indicator and the age indicator comprise the same plural bits.

12. (Previously Presented) A method of anonymously verifying an age or characteristic associated with a person associated with an identification document, the identification document including a document layer and printing carried by the document layer, the identification document further including a digital watermark embedded therein, the digital watermark including a first set of information, the first set of information including information to verify age or an age level of the person, the method comprising:

receiving optical scan data corresponding to the identification document, the optical scan data being generated by an optical sensor;

decoding the scan data with a configured multi-purpose electronic processor to obtain the first set of information included in the digital watermark, the first set of information including a concatenated string of data comprising an age indicator and additional data, wherein the digital

watermark is embedded in the identification document through hidden changes to data representing one or more items carried by the identification document; and

determining, based on the first set of information, the person's age or age level in connection with an age-related transaction or event, wherein said act of determining protects the anonymity of the person in possession of the identification document from said multi-purpose electronic processor or entity performing said determining.

13. Canceled.

14. (Original) The method of claim 12, wherein the identification document further comprises a second set of information embedded therein, the second set of information corresponding to a third set of information that is printed on the identification document, wherein the second set of information comprises an index for accessing a data repository.

15. (Original) The method of claim 14, wherein the index comprises a hash of the third set of information that is printed on the identification document.

16. (Previously Presented) The method of claim 14, further comprising computing a hash of the third set of information that is printed on the identification document, decoding the second set of information that is embedded in the identification document to obtain the embedded hash, and comparing the computed hash and the embedded hash to determine authenticity of the document.

17. (Previously Presented) The method of claim 12, further comprising storing at least a portion of the first set of information in at least one of a list, electronic memory circuits or a data record, wherein the stored portion of the first set of information serves as an audit clue to evidence that the identification document has been examined.

18. (Original) The method of claim 17, wherein the first set of information comprises two or more random bits.

19. (Original) The method of claim 18, wherein the first set of information comprises a date of birth.

20. (Original) The method of claim 19, wherein a combination of the random bits and the date of birth decrease likelihood of overlapping birth dates, while maintaining an anonymous audit clue.

21. (Withdrawn) A security document comprising:

a substrate; and

a first printed area carried by the substrate, the first printed area being steganographically encoded to secretly convey first plural bits of digital data recoverable by computer analysis of said first printed area, wherein the first printed area comprising an ink that is designed to degrade or rub off with use, thereby removing the steganographic encoding from the security document.

22. (Withdrawn) The method of claim 21, wherein the steganographic encoding comprises a digital watermark.

23. (Withdrawn) A security document comprising:

a substrate;

a first printed area carried by the substrate, the first printed area being steganographically encoded to secretly convey first plural bits of digital data recoverable by computer analysis of said first printed area; and

a second ink applied over the first ink in the first printed area, the second ink having a relatively lower adhesion property in comparison to the first ink, wherein the first plural bits of digital data are recoverable by computer analysis of the first printed area only after the second ink degrades or is removed from the security document.

24. (Withdrawn) The method of claim 23, wherein the steganographic encoding comprises a digital watermark.

25. (Previously Presented) A method comprising:

receiving optical scan data that is associated with an identification document, the identification document comprising plural-bits of data carried by the identification document, wherein the plural-bits of data comprise at least a first field and a second field, the first field carrying or linking to information corresponding to a bearer of the identification document and the second field corresponding to an age or age level of the bearer of the identification document;

utilizing a configured multi-purpose electronic processor, decoding the optical scan data to recover data corresponding to at least the second field;

receiving information carried by the document, separate from the data corresponding to at least the second field, and generating a reduced-bit representation of the received information by using a configured multi-purpose electronic processor; and

comparing data corresponding to the second field with the reduced-bit representation to verify an age level associated with of the document in connection with an age-related transaction or event,

wherein neither the data corresponding to the second field nor the reduced-bit representation betray the identity of the bearer of the identification document to said multi-purpose electronic processor or an entity performing said act of comparing.

26. Canceled.

27. (Previously Presented) The method of claim 25 further comprising storing the data corresponding to the second field in a data repository to evidence examination of the identification document.

28. (Previously Presented) The method of claim 25 further comprising printing the data corresponding to the second field to evidence examination of the identification document.

29. (Previously Presented) The method of claim 25, wherein said receiving information carried by the document comprises receiving data corresponding to at least one of data generated by a barcode scanner, optical character recognizer, manual entry or watermark decoder.

30. (Withdrawn) A method of embedding watermark information in an image captured by a digital camera, comprising:

capturing an image of a human subject;

identifying a face region in the captured image of the human subject;

realigning the captured image of the human subject within an image frame based at least in part on the identified face region; and

embedding the watermark information in the realigned captured image.

31. (Withdrawn) The method of claim 30 wherein realigning the captured image comprises centering the image within predetermined image frame dimensions.

32. (Withdrawn) The method of claim 30, wherein the realigning comprises identifying the human subject's silhouette.

33. (Withdrawn) The method of claim 32, wherein the embedding embeds the watermark information only in the silhouette.

34. (Withdrawn) The method of claim 32, wherein the embedding embeds a first watermark component only in the silhouette, and embeds a second watermark component only in an image area that does not correspond to the subject's silhouette.

35. (Withdrawn) The method of claim 34, wherein the second component comprises an orientation component.

36. (Withdrawn) The method of claim 34, further comprising embedding a third digital watermark component in artwork that is to be associated with the image.

37. (Withdrawn) The method of claim 30, wherein the digital camera comprises a video camera.

38. (Withdrawn) A method of embedding watermark information in an identification document, comprising:

receiving a digital image of a human subject, the digital image comprising a digital watermark embedded therein, wherein the digital watermark is designed to be removable from the image without significant image degradation, the digital watermark comprising a first set of information that is associated with the human subject;

removing the digital watermark from the digital image to obtain the first set of information;

embedding a second set of information in the digital image; and

printing the digital image on an identification document layer.

39. (Withdrawn) The method of claim 38, wherein the second set of information comprises the first set of information.

40. (Withdrawn) The method of claim 38, wherein the second set of information corresponds with the first set of information.

41. (Withdrawn) The method of claim 38, wherein the first set of information comprises an index, and said method further comprises interrogating a data repository with the index to access the second set of information.

42. (Withdrawn) The method of claim 41, wherein the data repository includes auxiliary information, wherein said embedding is controlled at least in part based on the auxiliary information.

43. (Withdrawn) The method of claim 38, wherein the first set of information comprises data to authenticate the digital image.

44. (Withdrawn) The method of claim 38, wherein the first set of information includes data to indicate a source of the digital image.

45. (Withdrawn) The method of claim 44, wherein the source comprises an image capture location.

46. (Withdrawn) The method of claim 44, wherein the source comprises a camera identifier.

47. (Withdrawn) The method of claim 44, wherein the source comprises a distribution trail.

48. (Withdrawn) An identification document comprising:

a substrate;

a first graphic carried by the substrate, the first graphic conveying a photographic image to human viewers thereof,

the first graphic being steganographically encoded to secretly convey first plural bits of digital data recoverable by computer analysis of said first graphic; and

a laminate layer provided over at least some of the substrate area that includes the first graphic,

wherein the laminate is steganographically encoded to secretly convey second plural bits of digital data recoverable by computer analysis of said laminate, wherein the second plural bits of digital data are steganographically encoded in a manner that differs from the steganographic encoding of the first plural bit of digital data.

49. (Withdrawn) The method of claim 48, wherein the steganographically encoded first plural bits of digital data and the steganographically encoded second plural bits of digital data cooperate to verify authenticity of the security document.

50. (Withdrawn) The method of claim 48, wherein the computer analysis of the first graphic is performed on data captured through optical scanning of the first graphic, and the computer analysis of the laminate is performed on data corresponding to the surface topology of the laminate.

51. (Withdrawn) The method of claim 48, wherein the laminate is encoded through varying the surface texture of the laminate.

52.-57. (Canceled)

58. (Previously Presented) An apparatus comprising:

a processor configured to:

receive first digital data corresponding to an age indicator, the first digital data being obtained from auxiliary data steganographically embedded in the document;

receive second digital data corresponding to a biometric indictor, the second digital data being obtained from auxiliary data steganographically embedded in the document;

receive third digital data corresponding to a biometric sample, wherein the biometric sample corresponds to the bearer; and

verify the bearer's age when: i) the first digital data indicates that the bearer is at least as old as a predetermined age, and ii) the second digital data and the third digital data correspond.

59. (Previously Presented) A non-transitory computer-readable medium having instructions stored thereon that, if executed by a computing device, cause the computing device to perform operations comprising:

receiving first digital data corresponding to an age indicator, the first digital data being obtained from auxiliary data steganographically embedded in the document;

receiving second digital data corresponding to a biometric indictor, the second digital data being obtained from auxiliary data steganographically embedded in the document;

receiving third digital data corresponding to a biometric sample, wherein the biometric sample corresponds to the bearer; and

verifying the bearer's age when: i) the first digital data indicates that the bearer is at least as old as a predetermined age, and ii) the second digital data and the third digital data correspond.

60. (Previously Presented) An apparatus comprising:

a processor configured to:

receive optical scan data corresponding to an identification document, the optical scan data being generated by an optical sensor, wherein the identification document is associated with a person, the identification document including a document layer and printing carried by the document layer, the identification document further including a digital watermark embedded therein, the digital watermark including a first set of information, the first set of information including information to verify age or an age level of the person;

decode the scan data to obtain the first set of information included in the digital watermark, the first set of information including a concatenated string of data comprising an age indicator and additional data, wherein the digital watermark is embedded in the identification document through hidden changes to data representing one or more items carried by the identification document; and

determine, based on the first set of information, the person's age or age level in connection with an age-related transaction or event, wherein said act of determining protects the anonymity of the person in possession of the identification document from the processor or and entity associated with said determining.

61. (Previously Presented) A non-transitory computer-readable medium having instructions stored thereon that, if executed by a computing device, cause the computing device to perform operations comprising:

receiving optical scan data corresponding to an identification document, the optical scan data being generated by an optical sensor, wherein the identification document is associated with a person, the identification document including a document layer and printing carried by the document layer, the identification document further including a digital watermark embedded therein, the digital watermark including a first set of information, the first set of information including information to verify age or an age level of the person;

decoding the scan data to obtain the first set of information included in the digital watermark, the first set of information including a concatenated string of data comprising an age indicator and additional data, wherein the digital watermark is embedded in the identification document through hidden changes to data representing one or more items carried by the identification document; and

determining, based on the first set of information, the person's age or age level in connection with an age-related transaction or event, wherein said act of determining protects the

anonymity of the person in possession of the identification document from the computing device or and entity associated with said determining.

62. (Previously Presented) An apparatus comprising:

a processor configured to:

receive optical scan data that is associated with an identification document, the identification document comprising plural-bits of data carried by the identification document, wherein the plural-bits of data comprise at least a first field and a second field, the first field carrying or linking to information corresponding to a bearer of the identification document and the second field corresponding to an age or age level of the bearer of the identification document;

decode the optical scan data to recover data corresponding to at least the second field;

receive information carried by the document, separate from the data corresponding to at least the second field, and generating a reduced-bit representation of the received information; and

compare data corresponding to the second field with the reduced-bit representation to verify an age level associated with of the document in connection with an age-related transaction or event,

wherein neither the data corresponding to the second field nor the reduced-bit representation betray the identity of the bearer of the identification document to the processor or an entity performing said act of comparing.

63. (Previously Presented) A non-transitory computer-readable medium having instructions stored thereon that, if executed by a computing device, cause the computing device to perform operations comprising:

receiving optical scan data that is associated with an identification document, the identification document comprising plural-bits of data carried by the identification document, wherein the plural-bits of data comprise at least a first field and a second field, the first field carrying or linking to information corresponding to a bearer of the identification document and the second field corresponding to an age or age level of the bearer of the identification document;

decoding the optical scan data to recover data corresponding to at least the second field;

receiving information carried by the document, separate from the data corresponding to at least the second field, and generating a reduced-bit representation of the received information; and

comparing data corresponding to the second field with the reduced-bit representation to verify an age level associated with of the document in connection with an age-related transaction or event,

wherein neither the data corresponding to the second field nor the reduced-bit representation betray the identity of the bearer of the identification document to the computing device or an entity performing said act of comparing.